Endpoint Protection

Mar 15, 2016 09:00 AM

Jon DiMaggio

View the indicators of compromise for this attack group.

Many security-minded organizations utilize code signing to provide an additional layer of security and authenticity for their software and files. Code signing is carried out using a type of digital certificate known as a code-signing certificate. The process of code signing validates the authenticity of legitimate software by confirming that an application is from the organization who signed it. While code-signing certificates can offer more security, they can also live an unintended secret life providing cover for attack groups, such as the Suckfly APT group.

In late 2015, Symantec identified suspicious activity involving a hacking tool used in a malicious manner against one of our customers. Normally, this is considered a low-level alert easily defeated by security software. In this case, however, the hacktool had an

unusual characteristic not typically seen with this type of file; it was signed with a valid code-signing certificate. Many hacktools are made for less than ethical purposes and are freely available, so this was an initial red flag, which led us to investigate further.

As our investigation continued, we soon realized this was much larger than a few hacktools. We discovered Suckfly, an advanced threat group, conducting targeted attacks using multiple stolen certificates, as well as hacktools and custom malware. The group had obtained the certificates through pre-attack operations before commencing targeted attacks against a number of government and commercial organizations spread across multiple continents over a two-year period. This type of activity and the malicious use of stolen certificates emphasizes the importance of safeguarding certificates to prevent them from being used maliciously.

An appetite for stolen code-signing certificates

Suckfly has a number of hacktools and malware varieties at its disposal. Figure 1 identifies the malware and tools based on functionality and the number of signed files with unique hashes associated with them.

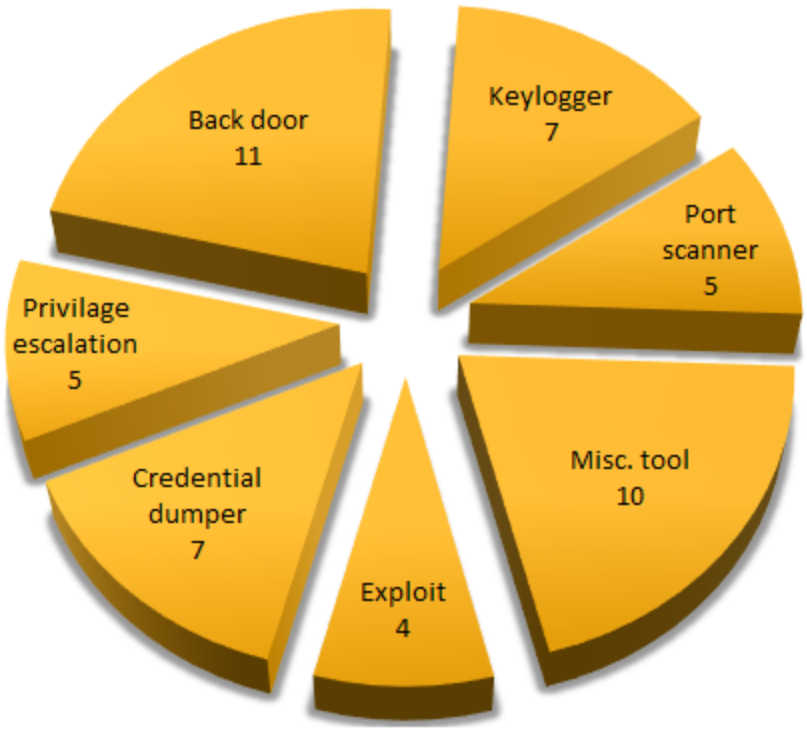

Figure 1. Suckfly hacking tools and malware, characterized by functionality

The first signed hacktool we identified in late 2015 was a digitally signed brute-force server message block (SMB) scanner. The organization associated with this certificate is a South Korean mobile software developer. While we became initially curious because the hacktool was signed, we became more suspicious when we realized a mobile software developer had signed it, since this is not the type of software typically associated with a mobile application.

Based on this discovery, we began to look for other binaries signed with the South Korean mobile software developer's certificate. This led to the discovery of three additional hacktools also signed using this certificate. In addition to being signed with a stolen certificate, the identified hacktools had been used in suspicious activity against a US-based health provider operating in India. This evidence indicates that the certificate's rightful owner either misused it or it had been stolen from them. Symantec worked with the certificate owner to confirm that the hacktool was not associated with them.

Following the trail further, we traced malicious traffic back to where it originated from and looked for additional evidence to indicate that the attacker persistently used the same infrastructure. We discovered the activity originated from three separate IP addresses, all located in Chengdu, China.

In addition to the traffic originating from Chengdu, we identified a selection of hacktools and malware signed using nine stolen certificates.

The nine stolen certificates originated from nine different companies who are physically located close together around the central districts of Seoul, South Korea. Figure 2 shows the region in which the companies are located.

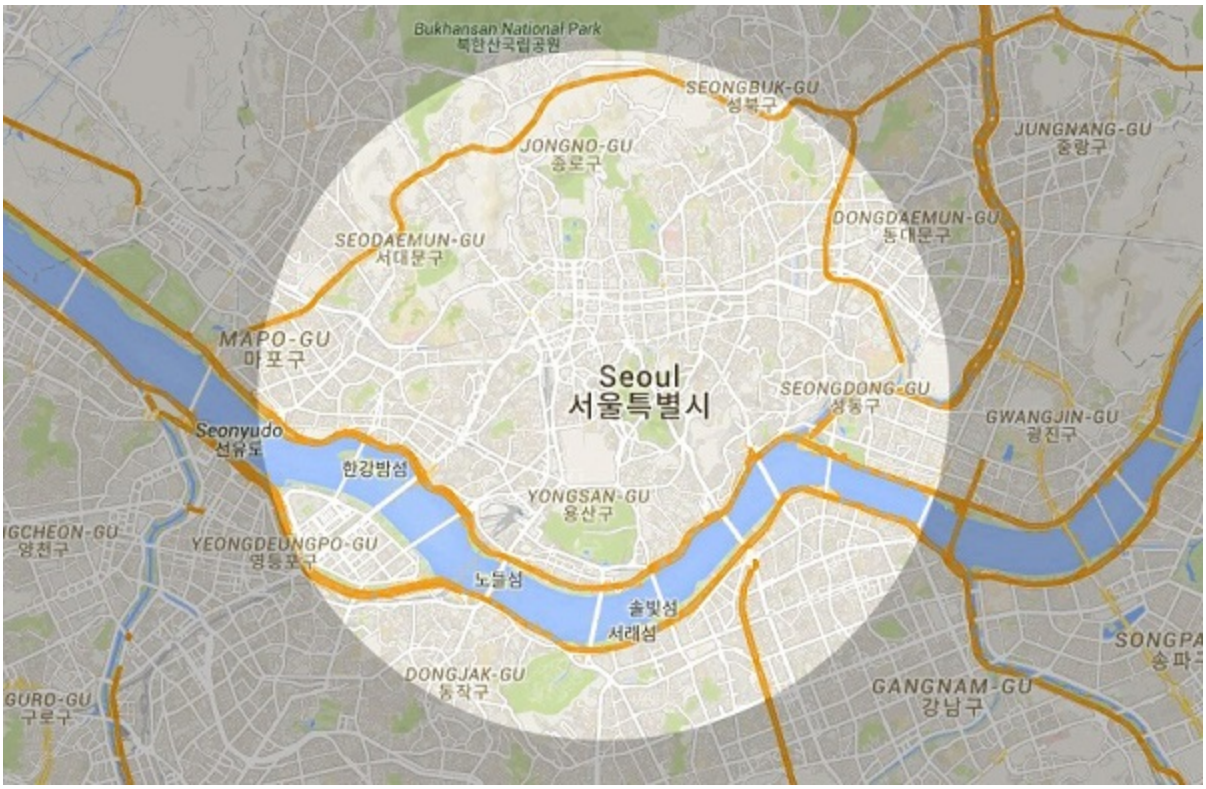

Figure 2. Map showing the central districts of Seoul, where the companies with the stolen certificates are located (Map data © 2016 SK planet)

While we do not know the exact circumstances of how the certificates were stolen, the most likely scenario was that the companies were breached with malware that had the ability to search for and extract certificates from within the organization. We have seen this capability

built into a wide range of threats for a number of years now.

The organizations who owned the stolen certificates were from four industries (see Figure 3).

Figure 3. Owners of stolen certificates, by industry

A timeline of misuse

We don't know the exact date Suckfly stole the certificates from the South Korean organizations. However, by analyzing the dates when we first saw the certificates paired with hacktools or malware, we can gain insight into when the certificates may have been stolen. Figure 4 details how many times each stolen certificate was used in a given month.

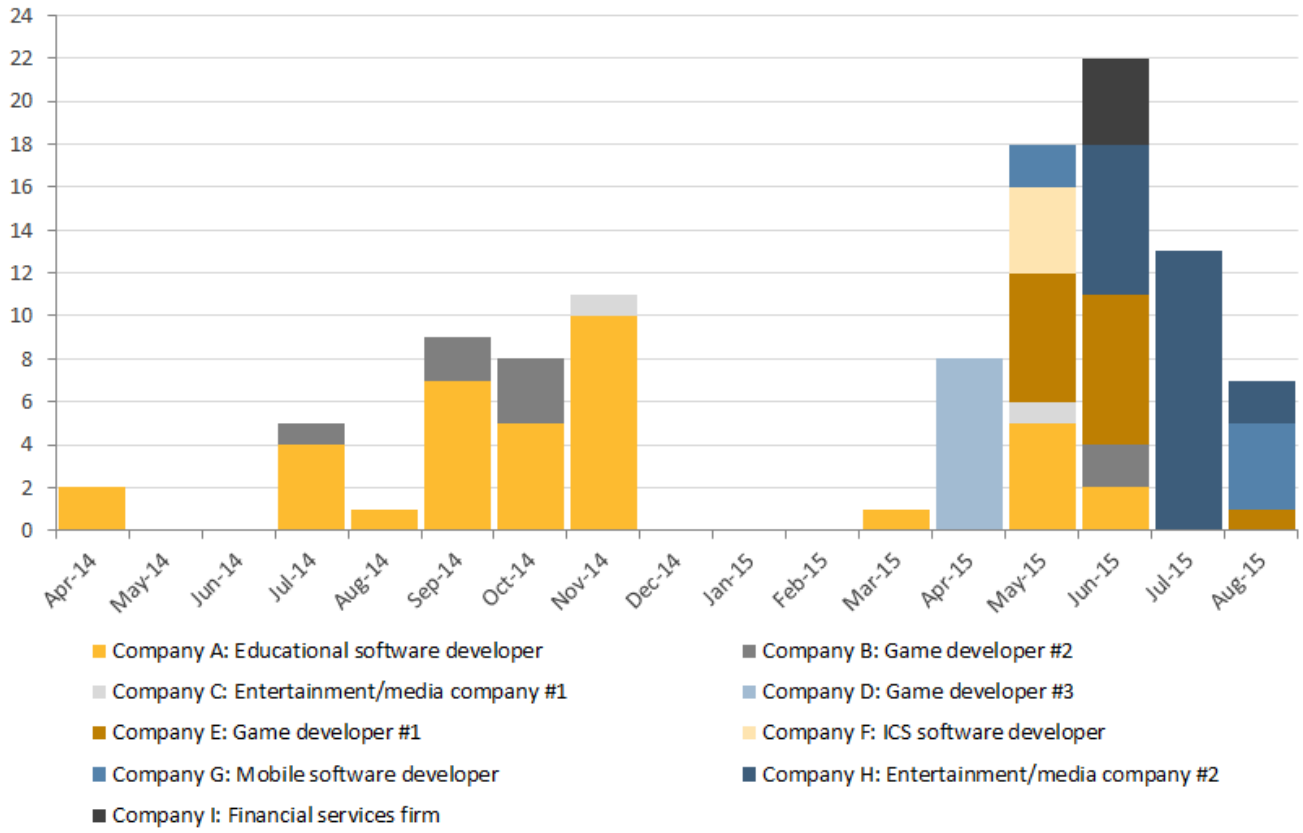

Figure 4. Tracking Suckfly's use of stolen certificates, by month

The first sighting of three of the nine stolen certificates being used maliciously occurred in early 2014. Those three certificates were the only ones used in 2014, making it likely that the other six were not compromised until 2015. All nine certificates were used maliciously in 2015.

Based on the data in Figure 4, the first certificates used belonged to Company A (educational software developer) and Company B (video game developer #2). Company A's certificate was used for over a year, from April 2014 until June 2015 and Company B's certificate was used for almost a year, from July 2014 until June 2015. When we discovered this activity, neither company was aware that their certificates had been stolen or how they were being used. Since the companies were unaware of the activity, neither stolen certificate had been revoked. When a certificate is revoked, the computer displays a window explaining that the certificate cannot be verified and should not be trusted before asking the user if they want to continue with the installation.

Signed, sealed, and delivered

As noted earlier, the stolen certificates Symantec identified in this investigation were used to sign both hacking tools and malware. Further analysis of the malware identified what looks like a custom back door. We believe Suckfly specifically developed the back door for use in cyberespionage campaigns. Symantec detects this threat as Backdoor.Nidiran.

Analysis of Nidiran samples determined that the back door had been updated three times since early 2014, which fits the timeline outlined in Figure 4. The modifications were minor and likely performed to add capabilities and avoid detection. While the malware is custom, it only provides the attackers with standard back door capabilities.

Suckfly delivered Nidiran through a strategic web compromise. Specifically, the threat group used a specially crafted web page to deliver an exploit for the Microsoft Windows OLE Remote Code Execution Vulnerability (CVE-2014-6332), which affects specific versions of Microsoft Windows. This exploit is triggered when a potential victim browses to a malicious page using Internet Explorer, which can allow the attacker to execute code with the same privileges as the currently logged-in user.

Once exploit has been achieved, Nidiran is delivered through a self-extracting executable that extracts the components to a .tmp folder after it has been executed. The threat then executes “svchost.exe”, a PE file, which is actually a clean tool known as OLEVIEW.EXE. The executable will then load iviewers.dll, which is normally a clean, legitimate file. Attackers have been known to distribute malicious files masquerading as the legitimate iviewers.dll file and then use DLL load hijacking to execute the malicious code and infect the computer. This technique is associated with the Korplug/Plug-x malware and is frequently used in China-based cyberespionage activity.

High demand for code-signing certificates

Suckfly isn’t the only attack group to use certificates to sign malware but they may be the most prolific collectors of them. After all, Stuxnet, widely regarded as the world’s first known cyberweapon, was signed using stolen certificates from companies based in Taiwan with dates much earlier than Suckfly. Other cyberespionage groups, including Black Vine and Hidden Lynx, have also used stolen certificates in their campaigns**.**

In April 2013, a third-party vendor published a report about a cyberespionage group using custom malware and stolen certificates in their operations. The report documented an advanced threat group they attributed to China. Symantec tracks the group behind this activity as Blackfly and detects the malware they use as Backdoor.Winnti.

The Blackfly attacks share some similarities with the more recent Suckfly attacks. Blackfly began with a campaign to steal certificates, which were later used to sign malware used in targeted attacks. The certificates Blackfly stole were also from South Korean companies, primarily in the video game and software development industry. Another similarity is that Suckfly stole a certificate from Company D (see Figure 4) less than two years after Blackfly had stolen a certificate from the same company. While the stolen certificates were different, and stolen in separate instances, they were both used with custom malware in targeted attacks originating from China.

Why do attackers want signed malware?

Signing malware with code-signing certificates is becoming more common, as seen in this investigation and the other attacks we have discussed. Attackers are taking the time and effort to steal certificates because it is becoming necessary to gain a foothold on a targeted computer. Attempts to sign malware with code-signing certificates have become more common as the Internet and security systems have moved towards a more trust and reputation oriented model. This means that untrusted software may not be allowed to run unless it is signed.

As we noted in our previous research on the Apple threat landscape, some operating systems, such as Mac OS X, are configured by default to only allow applications to run if they have been signed with a valid certificate, meaning they are trusted.

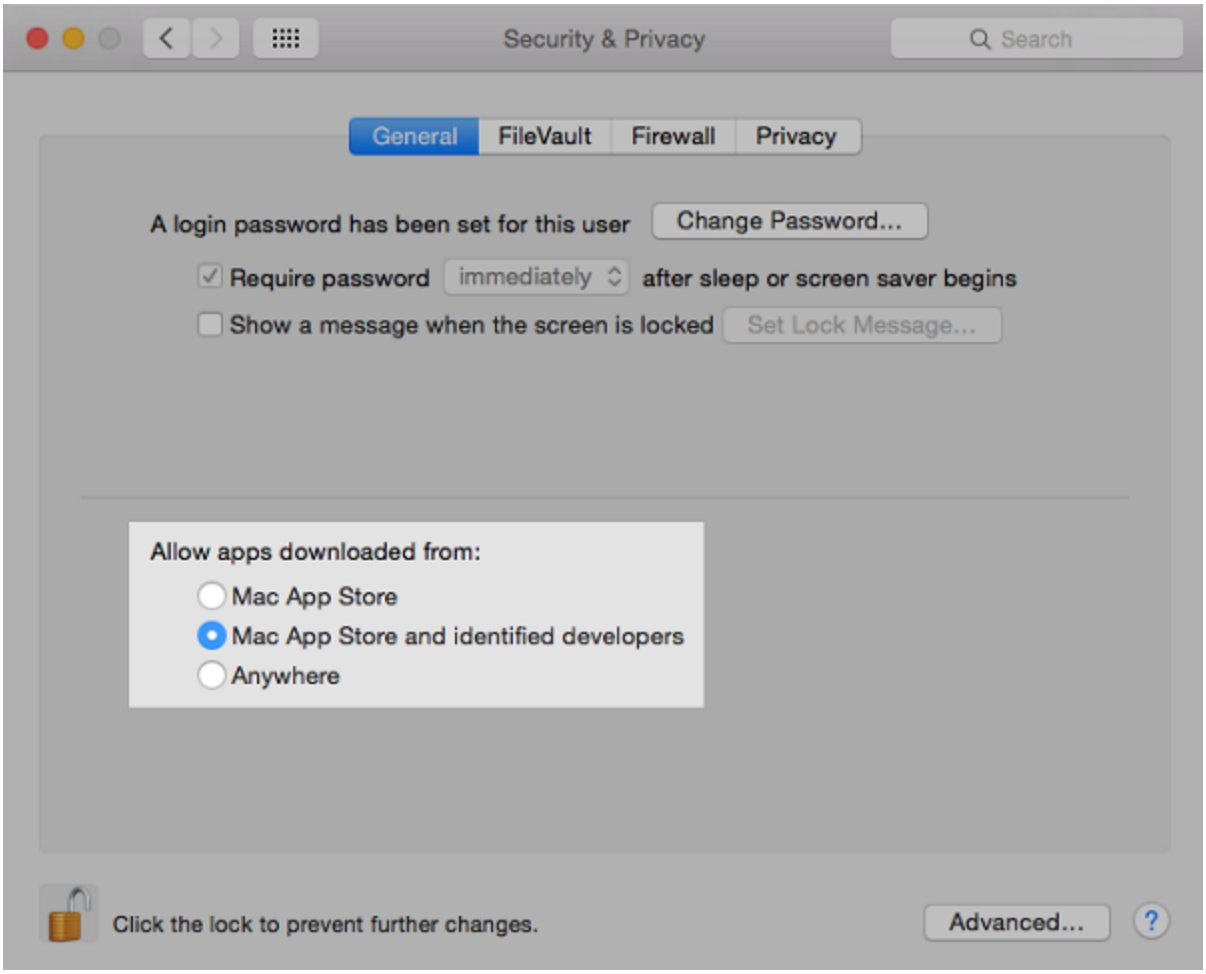

Figure 5. Mac OS X can be configured to only permit trusted apps to execute

However, using valid code-signing certificates stolen from organizations with a positive reputation can allow attackers to piggyback on that company's trust, making it easier to slip by these defenses and gain access to targeted computers.

Conclusion

Suckfly paints a stark picture of where cyberattack groups and cybercriminals are focusing their attentions. Our investigation shines a light on an often unknown and seedier secret life

of code-signing certificates, which is completely unknown to their owners. The implications of this study shows that certificate owners need to keep a careful eye on them to prevent them from falling into the wrong hands. It is important to give certificates the protection they need so they can't be used maliciously.

The certificates are only as secure as the safeguards that organizations put around them. Once a certificate has been compromised, so has the reputation of the organization who signed it. An organization whose certificate has been stolen and used to sign malware will always be associated with that activity.

Symantec monitors for this type of activity to help prevent organizations from being tied to malicious actions undertaken with their stolen certificates. During the course of this investigation, we ensured that all certificates compromised by Suckfly were revoked and the affected companies notified.

Over the past few years, we have seen a number of advanced threats and cybercrime groups who have stolen code-signing certificates. In all of the cases involving an advanced threat, the certificates were used to disguise malware as a legitimate file or application.

As this trend grows, it is more important than ever for organizations to maintain strong cybersecurity practices and store their certificates and corresponding keys in a secure environment. Using encryption, and services such as Symantec's Extended Validation (EV) Code Signing, and Symantec's Secure App Service can provide additional layers of security.

Protection
Symantec has the following detections in place to protect against Suckfly's malware:

Antivirus

Intrusion prevention system

Further information

- To learn more about Symantec's digital certificate solutions for code signing, please visit our Code Signing Information Center.
- To learn more about how best to protect your code-signing certificates, read our whitepaper: Securing Your Private Keys As Best Practice for Code Signing Certificates

Update – March 18, 2016

Indicators of compromise

File hashes

- 05edd53508c55b9dd64129e944662c0d
- 1cf5ce3e3ea310b0f7ce72a94659ff54
- 352eede25c74775e6102a095fb49da8c
- 3b595d3e63537da654de29dd01793059
- 4709395fb143c212891138b98460e958
- 50f4464d0fc20d1932a12484a1db4342
- 96c317b0b1b14aadfb5a20a03771f85f
- ba7b1392b799c8761349e7728c2656dd
- de5057e579be9e3c53e50f97a9b1832b
- e7d92039ffc2f07496fe7657d982c80f
- e864f32151d6afd0a3491f432c2bb7a2

Infrastructure

- usv0503[.]iqservs-jp.com
- aux[.]robertstockdill.com
- fli[.]fedora-dns-update.com
- bss[.]pvtcdn.com
- ssl[.]microsoft-security-center.com
- ssl[.]2upgrades.com
- 133.242.134.121
- fli[.]fedora-dns-update.com